UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/611,472	06/30/2003	Peter Szor	SYMC1034	1598

34350 7590 05/04/2007

GUNNISON, MCKAY & HODGSON, L.L.P.
1900 GARDEN ROAD, SUITE 220
MONTEREY, CA 93940

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
05/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/611,472	SZOR, PETER	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/8/03,2/26/07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 30 June 2003.

2. Claims 1-29 are pending for examination.

3. Claims 1-29 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Magdych et al, U.S. Patent No. 6,546,493 B1.

6. As per claim 1; "A method comprising:

detecting an attack by

malicious code on

a first computer system [Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas a system utilizing predetermined policy based intrusion/attack detection/risk assessment/remediation that is embodied in multiple processing elements (i.e., first/second computer systems) configured in a

network architecture, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

extracting a malicious code signature from

said malicious code [Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, and more particularly col. 3,lines 23-49, whereas the comparison of 'a plurality of virus/attack signatures ... or extract the harmful information from the infected communications ...' aspects of the intrusion/attack detection/risk assessment/remediation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

creating an extracted malicious code packet including

said malicious code signature [Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas the intrusion/attack detection/risk assessment/remediation that is embodied in multiple processing elements (i.e., separate intrusion/attack detection (first computer) system versus the risk assessment/remediation (second computer) system where the first to second extracted malicious code information clearly is transferred in a coded packet), clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and

sending said extracted malicious code packet from

said first computer system to

a second computer system [Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas the intrusion/attack detection/risk assessment/remediation that is embodied in multiple processing elements (i.e.,

separate intrusion/attack detection (first computer) system versus the risk assessment/remediation (second computer) system where the first to second extracted malicious code information clearly is transferred in a coded packet), clearly encompasses the claimed limitations as broadly interpreted by the examiner.].".

And further as per claim 27, this claim is an apparatus (system) claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; "A computer system comprising:

an intrusion prevention application for

detecting an attack by malicious code on

a first computer system;

a host signature extraction application for

extracting a malicious code signature from

said malicious code;

said host signature extraction application further for

creating an extracted malicious code packet including

said malicious code signature; and

said host signature extraction application further for

sending said extracted malicious code packet from

said first computer system to

a second computer system.".

7. Claim 2 ***additionally recites*** the limitations that; "The method of Claim 1 wherein prior to said sending, said method further comprising

determining that said extracted malicious code packet is

a new extracted malicious code packet.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas a system utilizing predetermined policy based intrusion/attack detection/risk assessment/remediation is such that the risk assessment aspect encompasses the initial (i.e., new) determination of an extracted malicious code/attack, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

8. Claim 3 ***additionally recites*** the limitations that; "The method of Claim 1 wherein prior to said sending, said method further comprising

determining that a maximum number of extracted malicious code packets have not been sent from

said first computer system.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas a system utilizing predetermined policy based intrusion/attack detection/risk assessment/remediation is such that the risk assessment aspect encompasses the threshold (i.e., maximum number) determination of an extracted malicious code/attack, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

9. Claim 4 ***additionally recites*** the limitations that; "The method of Claim 1 wherein said extracted malicious code packet is sent from

said first computer system to

said second computer system

on a secure channel.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas the intrusion/attack detection/risk assessment/remediation that is embodied in multiple processing elements (i.e., first computer/second computer) system where the first to second extracted malicious code information clearly is transferred across the Internet (i.e., WWW) such that the secure (i.e., SSL, HTTPS) aspects of secure Web communications, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

10. As per claim 5; "A method comprising:

detecting an attack by

malicious code on

a first computer system [Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas a system utilizing predetermined policy based intrusion/attack detection/risk assessment/remediation that is embodied in multiple processing elements (i.e., first/second computer systems) configured in a network architecture, clearly encompasses the claimed limitations as broadly interpreted by the examiner.];

creating an extracted malicious code packet including

parameters associated with

said malicious code [Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas the intrusion/attack detection/risk assessment/remediation that is embodied in multiple processing elements (i.e., separate intrusion/attack detection (first computer) system versus the risk assessment/remediation (second computer) system where the first to second extracted malicious code information (i.e., malicious code and network node communications support/address parameters and associated protocol information) clearly is transferred in a coded packet), clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and

sending said extracted malicious code packet from

said first computer system to

a second computer system [Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas the intrusion/attack detection/risk assessment/remediation that is embodied in multiple processing elements (i.e., separate intrusion/attack detection (first computer) system versus the risk assessment/remediation (second computer) system where the first to second extracted malicious code information clearly is transferred in a coded packet), clearly encompasses the claimed limitations as broadly interpreted by the examiner.].".

And further as per claim 28, this claim is an apparatus (system) claim for the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection; "A computer system comprising:

an intrusion prevention application for

detecting an attack by malicious code on

a first computer system;

a host signature extraction application for

creating an extracted malicious code packet including

parameters associated with said malicious code; and

said host signature extraction application further for

sending said extracted malicious code packet from

said first computer system to

a second computer system.".

11. Claim 6 ***additionally recites*** the limitations that; "The method of Claim 5 wherein prior to said sending, said method further comprising

determining that said extracted malicious code packet is

a new extracted malicious code packet.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas a system utilizing predetermined policy based intrusion/attack detection/risk assessment/remediation is such that the risk assessment aspect encompasses the initial (i.e., new)

determination of an extracted malicious code/attack, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

12. Claim 7 ***additionally recites*** the limitations that; "The method of Claim 5 wherein prior to said sending, said method further comprising

determining that a maximum number of extracted malicious code packets have not been sent from

said first computer system.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas a system utilizing predetermined policy based intrusion/attack detection/risk assessment/remediation is such that the risk assessment aspect encompasses the threshold (i.e., maximum number) determination of an extracted malicious code/attack, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

13. Claim 8 ***additionally recites*** the limitations that; "The method of Claim 5 wherein said extracted malicious code packet is sent from

said first computer system to

said second computer system

on a secure channel.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas the intrusion/attack detection/risk assessment/remediation that is embodied in multiple processing elements (i.e., first computer/second computer) system where the first to

second extracted malicious code information clearly is transferred across the Internet (i.e., WWW) such that the secure (i.e., SSL, HTTPS) aspects of secure Web communications, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

14. Claim 9 ***additionally recites*** the limitations that; "The method of Claim 5 further comprising

determining whether said malicious code is sendable.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas the extracted malicious code information by virtue of the fact that it is extracted from a file/resident in memory/cache memory, and can be transferred to the second computer across the network (i.e., 'sendable'), clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

15. Claim 10 ***additionally recites*** the limitations that; "The method of Claim 9 wherein upon a determination that said malicious code is sendable,

said method further comprising

extracting said malicious code from a memory location.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas the extracted malicious code information by virtue of the fact that it is extracted from a file/resident in memory ('from a memory location')/cache memory, and can be

transferred to the second computer across the network (i.e., 'sendable'), clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

16. Claim 11 ***additionally recites*** the limitations that; "The method of Claim 10 wherein said extracting comprises

copying or cutting said malicious code from

said memory location.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas the extracted malicious code information by virtue of the fact that it is extracted (i.e., 'copying or cutting') from a file/resident in memory ('from a memory location')/cache memory, and can be transferred to the second computer across the network (i.e., 'sendable'), clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

17. Claim 12 ***additionally recites*** the limitations that; "The method of Claim 10 further comprising

appending said parameters to

said malicious code after said extraction.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas the extracted malicious code information by virtue of the fact that it is extracted from a file/resident in memory ('from a memory location')/cache memory, and can be transferred to the second computer across the network (i.e., 'sendable' with associated

parameters), clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

18. Claim 13 ***additionally recites*** the limitations that; "The method of Claim 9 wherein upon a determination that said malicious code is not sendable,

said method further comprising

extracting a snippet of said malicious code from a memory location.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas in the case of the extracted malicious code information not extractable in its entirety (i.e., the process of 'extracting a snippet') from memory ('from a memory location')/cache memory, and therefore is assessed as not a 'complete' risk so assessable/acknowledgeable by the second computer, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

19. Claim 14 ***additionally recites*** the limitations that; "The method of Claim 13 wherein said extracting comprises

copying or cutting a portion of said malicious code from

said memory location.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas in the case of the extracted malicious code information not extractable in its entirety (i.e., the process of 'copying or cutting a portion of') from memory ('from a memory location')/cache memory, and therefore is assessed as not a 'complete' risk so

assessable/acknowledgeable by the second computer, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

20. Claim 15 ***additionally recites*** the limitations that; "The method of Claim 13 further comprising

appending said parameters to

said snippet after said extraction.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas in the case of the extracted malicious code information not extractable in its entirety (i.e., the process of 'copying or cutting a portion of') from memory ('from a memory location')/cache memory, and therefore is assessed as not a 'complete' risk so assessable (i.e., parts of/the snippet/the parameters)/acknowledgeable by the second computer, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

21. As per claim 16; "A method comprising:

receiving an extracted malicious code packet from

a first computer system with

a second computer system [Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas the intrusion/attack detection/risk assessment/remediation that is embodied in multiple processing elements (i.e., separate intrusion/attack detection (first computer) system versus the risk

assessment/remediation (second computer, 'receiving an extracted malicious code packet ...') system where the first to second extracted malicious code information clearly is transferred in a coded packet), clearly encompasses the claimed limitations as broadly interpreted by the examiner.]; and

determining whether an attack threshold

has been exceeded based upon

said extracted malicious code packet [Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas a system utilizing predetermined policy based intrusion/attack detection/risk assessment/remediation is such that the risk assessment aspect encompasses the threshold (i.e., maximum number) determination of an extracted malicious code/attack, clearly encompasses the claimed limitations as broadly interpreted by the examiner.].".

And further as per claim 29, this claim is an apparatus (system) claim for the method claim 16 above, and is rejected for the same reasons provided for the claim 16 rejection; "A computer system comprising:

a local analysis center signature extraction application for

receiving an extracted malicious code packet from

a first computer system with

a second computer system; and

said local analysis center signature extraction application further for

determining whether an attack threshold has been

exceeded based upon

said extracted malicious code packet.".

22. Claim 17 ***additionally recites*** the limitations that; "The method of Claim 16 wherein upon a determination that an attack threshold has been exceeded,

said method further comprising

delivering a signature update comprising

a malicious code signature.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, and more particularly col. 2,lines 27-55, whereas the comparison of '… a database of known vulnerabilities may then be updated based on risk assessment scan …' aspects of the intrusion/attack detection/risk assessment/remediation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

23. Claim 18 ***additionally recites*** the limitations that; "The method of Claim 17 wherein said signature update is delivered to

an intrusion detection system.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, and more particularly col. 2,lines 27-55, whereas the comparison of '… a database of known vulnerabilities may then be updated [i.e., at the 'intrusion detection system'] based on risk assessment scan …' aspects of the intrusion/attack detection/risk assessment/remediation, clearly

encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

24. Claim 19 ***additionally recites*** the limitations that; "The method of Claim 17 further comprising

determining that a maximum number of signature updates have

not been sent prior to said delivering a signature update.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, and more particularly col. 2,lines 27-55, whereas the comparison of '... a database of known vulnerabilities may then be updated [i.e., at the 'intrusion detection system'] based on risk assessment scan ...' aspects of the intrusion/attack detection/risk assessment/remediation, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

25. Claim 20 ***additionally recites*** the limitations that; "The method of Claim 17 further comprising

creating said signature update.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, and more particularly col. 2,lines 27-55, whereas the comparison of '... a database of known vulnerabilities may then be updated [i.e., at the 'intrusion detection system'] based on risk assessment scan ...' aspects of the intrusion/attack detection/risk assessment/remediation, clearly

encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

26. Claim 21 ***additionally recites*** the limitations that; "The method of Claim 16 wherein said extracted malicious code packet includes

a malicious code signature, and

wherein upon a determination that said attack threshold has been exceeded,

said method further comprising

delivering said malicious code signature to

a global analysis center.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas a system utilizing predetermined policy based intrusion/attack detection/risk assessment/remediation is such that the risk assessment aspect (i.e., at the risk assessment network element 'a global analysis center') encompasses the threshold (i.e., maximum number) determination of an extracted malicious code/attack, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

27. Claim 22 ***additionally recites*** the limitations that; "The method of Claim 21 further comprising

determining that a maximum number of malicious code signatures have

not been sent prior to

said delivering said malicious code signature.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas a system utilizing predetermined policy based intrusion/attack detection/risk assessment/remediation is such that the risk assessment aspect encompasses the threshold (i.e., maximum number) determination of an extracted malicious code/attack, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

28. Claim 23 ***additionally recites*** the limitations that; "The method of Claim 21 further comprising

extracting said malicious code signature from

said extracted malicious code packet.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas a system utilizing predetermined policy based intrusion/attack detection/risk assessment/remediation is such that the risk assessment aspect encompasses the extracted malicious code packet determination of an extracted malicious code/attack, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

29. Claim 24 ***additionally recites*** the limitations that; "The method of Claim 16 further comprising

determining whether said extracted malicious code packet includes

a malicious code signature,

wherein upon a determination that said extracted malicious code packet

does not include a malicious code signature, said method further comprising

extracting a malicious code signature from

said extracted malicious code packet.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas a system utilizing predetermined policy based intrusion/attack detection/risk assessment/remediation is such that the risk assessment aspect encompasses the extracted malicious code packet determination of an extracted malicious code/attack, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

30. Claim 25 ***additionally recites*** the limitations that; "The method of Claim 16 wherein upon a determination that

said attack threshold has been exceeded,

said method further comprising

delivering said extracted malicious code packet to

a global analysis center.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas a system utilizing predetermined policy based intrusion/attack detection/risk assessment/remediation is such that the risk assessment aspect (i.e., at the risk assessment network element 'a global analysis center') encompasses the threshold (i.e., maximum number) determination of an extracted malicious code/attack, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

31. Claim 26 ***additionally recites*** the limitations that; "The method of Claim 25 further comprising

determining that a maximum number of extracted malicious code packets

have not been sent prior to

said delivering said extracted malicious code packet.".

The teachings of Magdych et al (Abstract, figures 1-5 and associated descriptions, col. 2,lines 8-56, whereas a system utilizing predetermined policy based intrusion/attack detection/risk assessment/remediation is such that the risk assessment aspect (i.e., at the risk assessment network element 'a global analysis center') encompasses the threshold (i.e., maximum number) determination of an extracted malicious code/attack, clearly encompasses the claimed limitations as broadly interpreted by the examiner.) suggest such limitations.

Conclusion

32. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

5/2/07